TLDR

Background

The Components

- Group Policy Object All GPOs can be viewed using the Group Policy Management program found in the Server Manager suite. GPOs contains policies that affect Users or computers. The actual policies are stored on the Domain Controller, in the share called SYSVOL: ex: `\\contoso.local\sysvol\contoso.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}` Each GPO has a uniq GUID associated with it. A GPO can only apply to Users or Computers.
- Organizational Units (OU) OUs are just LDAP Containers, that can be used a little bit however you like. But it is usually used to logically group together Users, Groups or Computers. They are usually organized around geography (Country/City) or department (IT, Economy, HR, etc).
- GpLink GPOs can be linked to domains, sites, and OUs. For example, the default GPO is called `Default Domain Policy` and it is linked to the Domain Controller OU. The GpLink is stored on the LDAP entry that is linked to a GPO. So if you for example click on an OU, like the "Domain Controller" OU, you will see the attribute GpLink. The format of the “gplink” attribute value is `[<Distinguished name of the GPO>;<0 if the link is not enforced, 1 if the link is enforced>]`.

GPO Enforcement Logic

- GpLinks can be **enforced**, or not.
- OUs can **block inheritance**, or not.
- If a GpLink is enforced, the associated GPO will apply to the linked OU and all child objects, regardless of whether any OU in that tree blocks inheritance.
- If a GpLink is not enforced, the associated GPO will apply to the linked OU and all child objects, unless any OU within that tree blocks inheritance.

So a GpLink is always on, even though it says that it is not enforced.

The above mentioned rules apply to most scenarios. - WMI Filtering - You can further filter down to where a GPO is applied using "WMI-Filtering". To for example only apply the GPO to Windows 7 machines, or stuff like that. - Security Filtering - Filters so that an a GPO is only applied to specific users or computers.

So who can edit a GPO? It is just a simple ACL as any ACL on any other object. You can specify that a specific GPO can be edited by a specific user or group. The user that can edit that GPO can thus takeover users or computers that that GPO is applied to.

How to exploit

There are at least three different ways that an attacker can abuse GPOs to escalate privileges in a domain: - Who can create new GPOs in the domain. - Who can link GPOs to which OUs. - Who can modify existing GPOs (that may or may not be currently linked).

How to check for

You will want to check for ACLs that are between a low privileged user and a GPO can controls a high privileged object, such as a computer or user.

This cypher-query will check for user that Own GPOs.

```
match path=allShortestPaths((u:User {admincount: false})-[r]->(g:GPO)) return path
```

Check the default group policy called `Default Domain Controllers Policy`. Check the setting for `Allow Log On Locally`. If this is set to, for example, `Domain Users`, everyone in the domain has the permission to physically log on to the `Domain Controllers`. So if you have physical access to the DC you can just log in with a `Domain User` account.

Also check `Allow log on through Remote Desktop Services`.

If you don't have physical access you might be able to log on using a VM console, if that is enabled on the Domain Controller, or using an ILO.

This issue has been documented by Sean Metcalf here:

Recommendation

References

Seminal blogpost by Will Shroeder (HarmJoy) A must-read written by Wald0

Map out all GPO:s with powerview:

```
Get-NetGPO
```

1. Check which GPOs i have write access to

First find out which users that have access.

```
grep "IdentityReference" gpoer.txt > ident.txt
```

```
 grep -A 10 -i Autentiserade gpoer.txt
grep -A 10 -i "Domain users" gpoer.txt
```

2. Check which computer those GPO:s controls If I can have write access to a GPO that is applied to

Inte är standardgrupper Vilka användare har write